(iii) processing the stored information to create a second signature comprising a plurality of parameters related to the transmission of messages over a second period shorter than the first and more recent than the first;

(iv) updating the first signature by a weighted averaging with the second signature;

(v) detecting anomalies by inputting the signatures to the anomaly detector; and

(vi) processing the signatures using the anomaly detector to derive the anomalies by detecting unexpected patterns in the transmission of messages by the entity over the time period.

12. (four times amended) A computer system for detecting anomalies in messages transmitted over an electronic transmission medium by an entity comprising:

(i) a data store arranged to store information relating to the transmission of messages by the entity over a given time period,

(ii) an input arranged to receive information about each of a number of events which occurred during the time period;

(iii) a processor arranged to convert the information into a signature comprising a plurality of parameters related to the transmission of messages over the time period wherein the parameters comprise at least one parameter related to the transmission of messages over a portion of the period and also related to the position of the portion in the period, to enable output data to be derived from the stored information and wherein said processor is further arranged to convert at least part of the information into a second signature, comprising a plurality of parameters related to the transmission of messages over a second period, shorter than the first and more recent than the first; and also to update the first signature by a weighted averaging with the second signature;

(iv) an anomaly detector;

(v) an input arranged to provide the signatures to the anomaly detector; the anomaly detector being arranged to process the signatures to derive the anomalies by detecting unexpected patterns in the transmission of messages by the entity over the time period.

13. (four times amended) A method of deriving anomalies from messages transmitted electronically by an entity over an electronic transmission medium over time, comprising the steps of:

(i) creating a first signature comprising a plurality of parameters related to the transmission of messages over a predetermined first time period;

(ii) creating a second signature comprising a plurality of parameters related to the transmission of messages over a second period shorter than the first and more recent than the first;

(iii) updating the first signature by a weighted averaging with the second signature;

(iv) inputting the signatures to the anomaly detector; and

(v) detecting anomalies by processing the signatures using the anomaly detector to derive the anomalies by detecting unexpected patterns in the transmission of messages by the entity over the time period.

22. (four times amended) A computer system for detecting anomalies in messages transmitted by an entity over an electronic transmission medium over time, the system comprising:

an input arranged to receive information about the transmission of messages by the entity;

a processor arranged to create a first signature comprising a plurality of parameters related to the transmission of messages over a predetermined first time period and to create a second signature comprising a plurality of parameters related to the transmission of messages over a second period shorter than the first and more recent than the first;

a processor arranged to calculate a weighted averaging of the first and second signatures to form an updated first signature;

an anomaly detector;

an input arranged to provide the signatures to the anomaly detector; and

wherein said anomaly detector is arranged to process the signatures to derive the anomalies by detecting unexpected patterns in the transmission of message by the entity over the time period.

30. (amended) A method of detecting anomalous usage of a network comprising:-

(i) monitoring traffic flowing in the network,

(ii) processing the monitored traffic to generate a normal historic signature and a stored historic signature each representative of network usage over a first time period,

(iii) processing the monitored traffic to generate a current signature representative of network usage over a second time period which is shorter and more recent than the first time period,

(iv) comparing the current and normal historic signatures to determine whether the current signature represents normal usage,

(iv) if the current signature is determined to represent normal usage, producing an updated stored historic signature by combining the stored historic signature and the current signature using a weighted averaging procedure so that consistent trends present in the current signature are gradually over time introduced into the longer term trends incorporated in the stored historic signature,